5

10

15



CLAIMS

- 1. A method for block encryption of discrete data, comprising generating an encryption key in the form of a set of subkeys, breaking down a data block into N≥2 subblocks and alternate converting said subblocks by performing a dual-locus operation on on the subblock and the subkey, characterised in that prior to carrying out said dual-locus operation on i-th subblock and subkey, a conversion operation is performed on the subkey depending on j-th subblock, where j≠i.
- 2. A method according to claim 1, characterised in that an operation of permuting subkey bits depending on said j-th subblock is used as the j-th subblock-dependent conversion operation.
- 3. A method according to claim 1, characterised in that an operation of cyclic offsetting subkey bits depending on said j-th subblock is used as the j-th subblock-dependent conversion operation.
- 4. A method according to claim 1, characterised in that a substitution operation performed on a subkey depending on said j-th subblock is used as the j-th subblock-dependent conversion operation.